

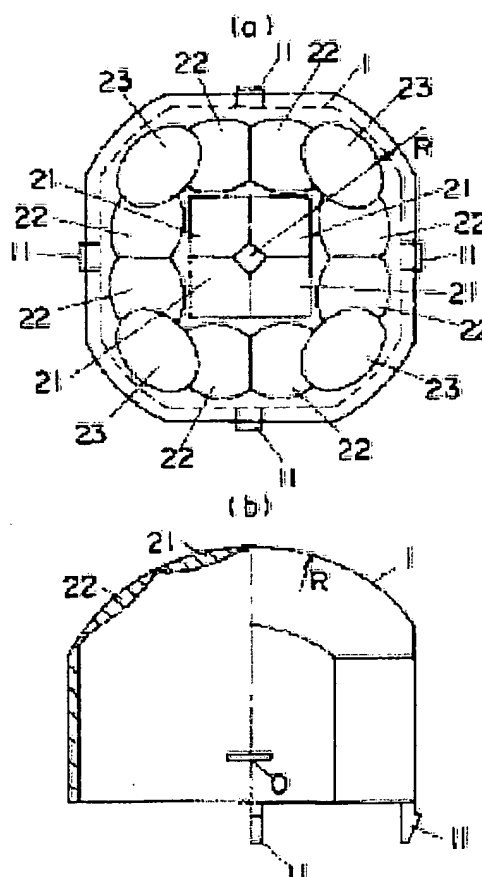
## DOME TYPE MULTI-LENS

**Patent number:** JP6242304  
**Publication date:** 1994-09-02  
**Inventor:** KAMIYA FUMIHIRO; IGARI MOTOO; HIMESAWA HIDEKAZU  
**Applicant:** MATSUSHITA ELECTRIC WORKS LTD  
**Classification:**  
**- international:** G01J1/02; G01J1/04; G02B3/08; G01J1/02; G01J1/04; G02B3/08; (IPC1-7): G02B3/08; G01J1/02; G01J1/04  
**- european:**  
**Application number:** JP19930029056 19930218  
**Priority number(s):** JP19930029056 19930218

Report a data error here

### Abstract of JP6242304

**PURPOSE:** To efficiently converge light from many directions. **CONSTITUTION:** In a dome type multi-lens obtained by arraying many lenses like a dome 1, respective lenses whose focuses are arranged on the center of the spherical outer surface of the dome 1 are formed by spherical lenses 21 to 23 and the areas of spherical lenses arranged on the periphery of the spherical lens arranged on the center part of the dome 1 are increased.



Data supplied from the esp@cenet database - Worldwide

## ⑫ 特 許 公 報 (B 2)

昭62-42304

⑤Int. Cl. <sup>4</sup>	識別記号	庁内整理番号	⑭公告	昭和62年(1987)9月8日
G 06 F 12/14	3 2 0	B-7737-5B		
9/06	3 3 0	A-7361-5B		
12/00	3 0 2	6711-5B		発明の数 2 (全6頁)

⑯発明の名称 ファイル呼出し機密の保護方法および装置

⑰特 願 昭59-42796

⑱公 開 昭59-169000

⑲出 願 昭59(1984)3月6日

⑳昭59(1984)9月22日

優先権主張 ㉑1983年3月7日㉒米国(US)㉓472609

㉔発 明 者	マーチン・エム・アタ ラ	アメリカ合衆国カリフォルニア州94025アサートンモン テ・ヴィスタ・アヴェニュー18
㉕出 願 人	アトラ・コーポレーシ ョン	アメリカ合衆国カリフォルニア州95131サン・ホセ・ペー リング・ドライヴ2363
㉖代 理 人	弁理士 古 谷 肇	
審 査 官	吉 岡 浩	

1

2

## ⑰特許請求の範囲

1 メモリ内のデータファイルの呼出しを制御する方法において、ファイルデータが複数の暗号化キーコードの最初のコードとの選択された論理組合せとして暗号化され、メモリの選択されたファイルアドレス位置に暗号化形態として記憶されてファイルデータを形成する段階と；各選択されたファイルアドレス位置に対する呼出し及びファイルデータと共にアドレス位置において暗号化される複数の暗号化キーコードのうちの1コードを記録する段階と；選択されたファイルアドレス位置におけるファイルデータ呼出し要求を、該ファイルデータに関連する暗号化キーコードを記録から判断することにより処理する段階と；選択されたファイルアドレス位置のファイルデータを前記の関連する暗号化キーコードを使用して脱暗号化する段階と；前記選択されたファイルアドレス位置用のファイルデータを前記選択された論理組合せ内における前記複数の暗号化キーコードの新しい1コードを使用して再度暗号化する段階と；新たに再度暗号化されたファイルデータを呼出ししたファイルアドレス位置において記憶する段階と；及び選択されたファイルアドレス位置への後の呼出し及び該呼出しと関連する新しい暗号化キーコードを指示するように前記記録を修正する段階とからなることを特徴とする方法。

2 選択されたファイルアドレス位置のファイルデータは、該選択されたファイルアドレス位置が以前呼出されていないという記録の判断にตอบสนองして、最初の暗号化キーコードを使用して脱暗号化されることを特徴とする、特許請求の範囲第1項記載の方法。

3 利用者の呼出し権限ファイルが備えられ、選択されたファイルアドレス位置を呼出す前に、前記ファイルから、該選択されたファイルアドレス位置を呼出し得る利用者の権限を判断する段階を備えることを特徴とする、特許請求の範囲第1項記載の方法。

4 選択されたファイルアドレス位置を事後に呼出し得る利用者の呼出し権限を、前記選択されたファイルアドレス位置のファイルデータのメモリ内への再暗号化にตอบสนองして、選択的に変化させる段階を備えることを特徴とする、特許請求の範囲第3項記載の方法。

5 前記記録から判断された暗号化キーコードを使用して、選択されたファイルアドレス位置の各々においてファイルデータの脱暗号化を行うこと、及び複数のキーコードの新しい最初の1コードを使用して、前記選択されたファイルアドレス位置の各々に前記ファイルデータを再暗号化することにより、全ファイルの初期状態再設定を行う段階を備えることを特徴とする、特許請求の範囲

3

4

第1項記載の方法。

6 以前に呼出されたという記録のないファイルアドレス位置のファイルデータの脱暗号化は、最初の暗号化キーコードを使用して行われることを特徴とする、特許請求の範囲第5項記載の方法。

7 ファイルデータを該ファイルデータと複数の暗号化キー信号のうちから選択された1信号との論理組合せとして暗号化して、選択されたファイルアドレスとして記憶する段階と；選択ファイルアドレス位置におけるファイルデータを前記論理組合せに従つて、前記ファイルデータと関連する暗号化キー信号を用いて脱暗号化する段階と；脱暗号化したファイルデータを新しい暗号化キー信号との論理組合せとして再度暗号化し、対応するファイルアドレス位置に記憶させる段階と；及び少なくとも選択されたファイルアドレス位置の各々を脱暗号化した回数と、該選択されたファイルアドレス位置の各々でファイルデータを再度暗号化し、且つ再度記憶した暗号化キー信号を示す情報を編集したものとしてファイル呼出記録を生成する段階とを備えることを特徴とする、特許請求の範囲第1項記載のファイル呼出し記録の形成方法。

8 選択可能なファイルアドレス位置を有するメモリ内に暗号化形態でファイルデータが記憶され、及び加えられた暗号化キー信号に回答して暗号化装置がファイルデータを暗号化するところの、無権限呼出しに対してファイルデータの機密保護を行う装置において；選択されたファイルアドレス位置に対して、ファイルデータと暗号化キー信号発生装置から加えられたキー信号との論理コード化組合せとして暗号化されたファイルデータを供給する暗号化装置と；選択されたファイルアドレス位置を指示し、ファイルデータ内部に記憶された該ファイルデータの暗号化と関連するキーコード信号を生成する記録装置と；選択されたファイルアドレス位置の識別に回答して前記記録装置からの関連する暗号化キー信号を判断し、関連する暗号化キー信号を供給するように前記キーコード発生装置を設定する第1の回路と；前記キーコード発生装置からの暗号化キー信号及びメモリからの暗号化されたファイルデータを受信するように配設され、且つ前記論理コード化組合せに従つて操作され、前記選択されたファイルアドレ

ス位置のファイルデータの脱暗号化を行う脱暗号化装置と；及び前記第1の回路は選択されたファイルアドレス位置に新しい暗号化キー信号と共に新たに暗号化されたファイルデータを再度記憶するための新しい暗号化キー信号を前記暗号化装置に供給するように前記キーコード発生装置を変更し、且つ選択されたファイルアドレス位置においてファイルデータと関連する新しい暗号化キー信号の指示を形成するように記録装置を変化させることを特徴とする装置。

9 前記第1の回路が、選択されたファイルアドレス位置の呼出しを以前に行つたことがないという前記記録装置の表示に回答して、キーコード発生装置を設定して、脱暗号化装置に対し最初の暗号化キー信号を供給することを特徴とする特許請求の範囲第8項記載の装置。

10 前記記録装置内のファイルデータを選択的に呼出す使用者の権限を表すデータを記憶する呼出し記録装置と、使用者からの識別データを受信するように配設され且つ前記回路に連結され、キーコード発生装置が無権限と識別された使用者について、前記脱暗号化装置へ暗号化キー信号を供給することを阻止する阻止手段とを備えることを特徴とする特許請求の範囲第8項記載の装置。

11 前記第1の回路が、選択されたファイルアドレス位置に新しい暗号化キー信号で新たに暗号化されたファイルデータが再度記憶されるのに応答して、前記呼出し記録装置内の前記選択されたファイルアドレス位置を呼出す使用者の識別された権限を変更することを特徴とする、特許請求の範囲第10項記載の装置。

12 キーコード発生装置、暗号化装置、脱暗号化装置及び記録装置に連結され、前記記録装置により定められたキーコード発生装置からの各々のファイルアドレス位置のための暗号化キー信号を用いて各々のファイルアドレス位置にあるファイルデータを選択的に脱暗号化するよう前記発生装置をセットし、新しい最初の暗号化キー信号を使用して各ファイルアドレス位置について脱暗号化したファイルデータを再度暗号化し、それぞれのファイルアドレス位置にて再度記憶させる初期条件設定装置を備えることを特徴とする、特許請求の範囲第8項記載の装置。

13 前記初期条件設定装置は、選択したファイ

ルアドレス位置を以前呼出したことがないという前記記録装置からの指示に応答して最初の暗号化キー信号を使用して当該ファイルデータの脱暗号化を行い、且つ新しい最初の暗号化キー信号を使用して脱暗号化されたファイルデータを再度暗号化し、それぞれのファイルアドレス位置にて新しく暗号化したファイルデータを再度記憶することを特徴とする、特許請求の範囲第12項記載の装置。

#### 発明の詳細な説明

機密データファイルについてコンピュータ制御の操作を行なう多くの公知の方法が存在する。これらにおいてはデータ（通常は暗号化された形態）を呼出す前に、ファイルを呼出そうとしている者の識別性を検証することを要する（例えば米国特許第3938091号、第3587051号、第3611293号及び第4198619号参照）。更に、クレジットカードに関係するものを含む公知の記録機密保護体系の多くは、使用する者が権限を有するか、及び記録中のデータが真実であるかどうかの双方を共に検証し、権限のない者の使用及び偽造又は複製記録を防止することを必要とする。この種の体系としては、米国特許第4304990号、第4328414号及び第4357429号に開示されたものがある。

上記形式のコンピュータ制御機密保護体系に関する1つの不具合は、その機密保護した記録を呼び出した者が誰であるか、ファイルには何の記録も残らないということである。

本発明の好適実施態様に従うと、最初、及びその後機密保護した暗号化ファイルと呼出すすべての場合に使用された暗号化制御キーの動的記録が、暗号化ファイルに対するあらゆる呼出しを監査する目的で、呼出し体系の能動要素及び機密保護した経歴の記録として形成される。更に、単に変更を伴わないディスプレイ上への表示だけのためであつたとしても、ファイルが一旦呼出されたなら、旧ファイルの置換が防止される。これによつて、一旦呼出されて、機密保護が危くなつたファイルは再度、複写、置換及び再使用に対し機密保護される。この形式の体系は特に銀行業、預金出納の操作について有用である。これは、例えば預金を引出すための口座ファイルへの最初の呼出しを慎重に制御し、正確な呼出しが行われるようにして、同一操作を何度も反復し、又当初の差引

残高をファイル内に置換するという面倒な操作を避けることができる。更に本発明により形成される、ファイルに対する呼出しの経歴記録は、該呼出しについて暗号化形態による監査記録を形成する。

以下、本発明の好適実施態様について、添付図面を参照しながら、詳細に説明する。

第1図を参照すると、中央処理装置（CPU）11、キーボード制御装置13及び記憶ファイル用の記憶手段（メモリ）15、17を備える典型的なコンピュータ・システムに呼出し機密保護モジュール9を付加した本発明によるブロック図が示してある。該メモリ15、17は半導体メモリ、鉄心状の磁気メモリ、クリスタル、ディスク、ドラム又はテープ若しくはこれらを任意に組合わせた型式の従来技術を使用して、メモリ17には呼出しを制御すべきデータを記憶し、且つ該記憶データ17を呼出すことのできる個人や機関についての呼出し権限情報をメモリ15に記憶することができる。キーボード13は従来の方法で、コンピュータシステムに対し手動入力呼出しを行なうもので、別のコンピュータシステム等を使用するような他のコンピュータ呼出し体系に普通に使用されているものである。

本発明によると、上記のような一般的なコンピュータシステムは修正されて、コンピュータシステムにより作動し、ファイルの呼出し毎にメモリ17に記憶されたデータを段階的に再暗号化し、場合によつては許可された権限に従つて、記憶手段15に記録させた呼出し権限情報を新らしく、且つ記憶手段17から呼出した各ファイルの脱暗号化及び再暗号化のために使用した暗号化キーについて暗号化形態による経歴ファイルを形成する呼出し機密保護モジュール9を備えるようにすることができる。更に、該モジュール9はメモリ17が記憶したファイルの多数の呼出しについて権限を確認した後、制御された初期状態再設定モードにて作動し、メモリ17の全てのファイルを新しい標準暗号化キーに復旧する。この初期状態再設定を行なう必要のある呼出し回数はモジュール9内の記憶容量如何によつて定まる。

第1図に加えて、第2図及び第3図を参照すると、第1図のシステムが中央処理装置14の制御のもとで作動する状態を示したフロー・チャート

及びブロック図がそれぞれ示してある。作動方法について説明すると、特定ファイルと呼出そうとする個人や機関Rはキーボード13を介して、個人識別番号(PIN)、特定ファイルに関する情報等を入力する。場合によつては、個人の識別検証ルーチン21を従来の方法にて実行し(例えば、米国特許第3938091号又は第4198619号に開示されているように)、又要求されたファイルと呼出す権限の有無について、呼出し権限ファイル15を調査することもできる。メモリ17内のファイルは全て最初にキーコード発生装置23からのキーコード $K_0$ と共に、暗号化モジュール21内にファイルデータを暗号化することにより、従来の方法(例えば、全国標準局(NBS)から入手可能であるデータの暗号化用標準(DES)モジュールを使用する方法)で暗号化される。

定められた権限25によつて、特定のファイル#Xと呼出することができるが、該ファイル#Xを脱暗号化するには正確なキーコードを必要とする。この目的上、後で詳しく説明するキー使用制御ファイル19が調査され、該ファイル#Xが以前に呼出されたか否かを判断する。このため、以前の呼出し状態、即ち、該ファイル#Xの呼出を以前に行なつたか否かを知ることが可能となる。以前に呼出しを行なっていない場合は、該ファイル#Xはキー使用制御ファイルに現れない。このことは、ファイル#Xが最初のキーコード $K_0$ で暗号化した状態で記憶手段17に現れることを示すものである。キー発生装置23は連続した相異なるキーコード $K_0, K_1, K_2, K_3, \dots, K_n$ を生成することができるが、この場合にはキーコード $K_0$ を脱暗号化モジュール27(これは当然DESモジュールと同一型式、もしくは暗号化モジュール21と同一のモジュールとすることができる)に

35 対し供給できるよう設定する。従つて、要求されたファイル#Xはキーコード $K_0$ を使用して、従来の方法で脱暗号化され、明確な文章にて、呼出しデータ29を提供することができる。次いで、データは販売、預金、引出し等のようなデータ使用による処理を反映する新しいデータ変更31を伴つて、もしくは伴わずに、記憶手段に戻され、新しいキーコード $K_1$ を使用して、暗号化形態にて再記憶される。これは、キーコード発生装置23を設定器38により再設定し、暗号化モジュール21にキーコード $K_1$ を供給し、変更された或いはされないデータ33をモジュール21内でキーコード $K_1$ と共に暗号化を行なうことにより行われ得る。更に、キー使用制御ファイル19は新しくされて、ファイル#Xが以前に呼出されており、連続するキーコード $K_1$ と共に新しく暗号化された状態にてメモリに記憶されていることを示すようになる。更に、場合によつては呼出し権限ファイル15が新しくされ、例えば利用者Rによるファイル#Xの呼出しが「新しい日付」まで、又は別の利用者に呼出されるまで禁止されるなどすることができる。連続的に権限を認めることができるならば、その後の利用者R、又は別の利用者によるファイル#Xの呼出しはキーコード $K_1$ による暗号化を介して行なわなければならない。

以前にファイル#Xが呼出されている場合には、キー使用制御ファイル19は以前のファイル#Xの呼出し回数によつて、以前に呼出され且つ新しいキーコード $K_1, K_2, \dots, K_n$ で暗号化された状態でメモリに戻されたファイル#Xの入力を保持している。このようにして、ファイル#Xがファイル#00100番地に存在するとした場合における、キー使用制御ファイル19の典型的状態を図示する第4図のチャートを参照すると、このファイルに対する以前の呼出しはキーコード $K_2$ で(37において)再暗号化した状態にて再記憶されていることが判る。キー使用制御ファイル19を調査すると、ファイル#00100は以前に2回呼出されて、現在は脱暗号化のためにキーコード $K_2$ を必要としていることが判る。利用者の権限が依然として正当であることが呼出権限39から判明すると、キーコード発生装置23は脱暗号化モジュール27に対しキーコード $K_2$ を供給し、このファイル中のデータを明確な文章29にて提供

35 供するよう設定される。このファイルからのデータを修正又は未修正の形態にて再記憶することは、設定器38によりキーコード発生装置23を再設定して、キーコード $K_3$ (第4図の41)の暗号化モジュール21内への供給を行ない、そこで新しい該キーコード $K_3$ を使用して、戻されたデータを暗号化することによつて行われる。メモリ17内のデータの検索は全て、アドレスファイル内の情報を破壊読出しすることによつて行なうことができ、従つて、そこに再記憶させるデータ

9

10

は新しい暗号化形態にて書き込むことができる。メモリ 17 内で多くの呼出しを行なった後、キー使用制御ファイル 19 は一般に、第 4 図に示すような入力を備える。該ファイルは選択的に各ファイルの呼出しを行なった特定の利用者を識別し得るコードをも備えることができる。このようにしてファイル 19 はメモリ 17 内のファイルの呼出しに対する監査記録を提供する。更に、キー使用制御ファイル 19 はメモリ 17 内のデータ及び、メモリ 17 内のデータを脱暗号化するに必要な実際のキーコード  $K_1, \dots, K_n$  (発生装置 23 によつてのみ生成) を絶対に漏洩しないため、暗号化された形態を保つ。更に、ファイル保護コードとして作用するキーコード  $K_0, \dots, K_n$  は従来の方法、例えば乱数発生プログラムを用いることにより、発生装置 23 内部で発生することができ、従つて、誰にも知らせる必要がない。

任意の特定ファイルに対する連続キーコードの限界近くまで、メモリ 17 内のデータを何回も、又は定期的に呼出しした後、メモリ 17 内の全収集ファイルは中央処理装置 14 の制御に基づいて、第 3 図に示した装置を使用して、連続新キーコード  $K'_0, K'_1, \dots, K'_n$  の最初のキーコード  $K'_0$  により再暗号化することができる。しかし、メモリ

17 内のファイルは異なるキーコードで暗号化してあるため、新しい最初のキーコード  $K'_0$  で再度暗号化するためにまず各ファイル中のデータを脱暗号化するについてどのキーを使用すべきかを判断するのに、キー使用制御ファイル 19 に問合せする必要がある。この初期条件再設定の作動完了後、連続キーコード  $K_0, \dots, K_n$  用のキー使用制御ファイル 19 をリタイヤさせ、新しい暗号化コードの下でコンピュータシステム又はメモリ 7 内のデータの機密保護を損うことなく、メモリ 17 内のデータに対する呼出し経歴の記録とすることができる。

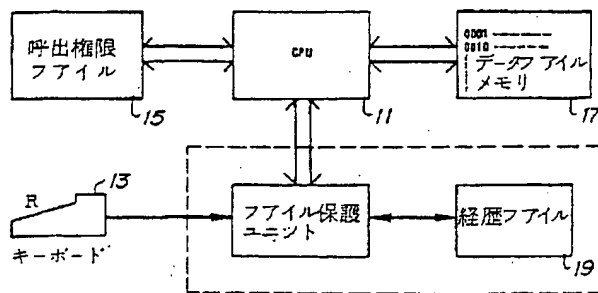
#### 図面の簡単な説明

第 1 図は本発明の装置の一実施態様を示したブロック図、第 2 図は第 1 図の装置の作動状態を示したフロー・チャート、第 3 図は本発明の説明した実施態様のブロック図、及び第 4 図は本発明によるキー使用制御ファイルの形態と作用を示すチャート図である。

9…呼出し機密保護モジュール、11、14…中央処理装置 (CPU)、13…キーボード制御装置、15、17…メモリ、19…経歴ファイル、21…暗号化モジュール、23…キーコード発生装置。

キーコード	$K_1$	$K_2$	$K_3$	$K_4$	-----	$K_M$
ファイル番号						
01001	*					
11010				*		
00001	*					
00100						
00110						*
...						
10110						*

第 4 図



第 1 図

